F. No. 2(22)/2013-EG-II
Ministry of Communication & Information Technology
Department of Electronics & Information Technology

E-mail Policy

Of

Government of India

October 2014
Version 1.0

Department of Electronics and Information Technology
Ministry of Communications and Information Technology
Government of India
New Delhi - 110003

Table of Contents

1. Introduction

1.1 The Government uses e-mail as a major mode of communication. Communications include Government of India (GoI) data that travel as part of mail transactions between users [1] located both within the country and outside.

1.2 This policy of Government of India lays down the guidelines with respect to use of e-mail services. The Implementing Agency (IA) [2] for the GoI e-mail service shall be National Informatics Centre (NIC), under the Department of Electronics and Information Technology (DeitY), Ministry of Communications and Information Technology. The organisations exempted under Clause 14 will themselves become the Implementing Agency (IA) for the purpose of this policy.

2. Scope

2.1 Only the e-mail services provided by NIC, the Implementing Agency of the Government of India shall be used for official communications by all organizations except those exempted under clause no 14 of this policy. The e-mail services provided by other service providers shall not be used for any official communication.

2.2 This policy is applicable to all employees of GoI and employees of those State/UT Governments that use the e-mail services of GoI and also those State/UT Governments that choose to adopt this policy in future. The directives contained in this policy must be followed by all of them with no exceptions. All users of e-mail services can find further information in the supporting policies available on http://www.deity.gov.in/content/policiesguidelines under the caption “E-mail Policy”.

2.3 E-mail can be used as part of the electronic file processing in Government of India. Further information in this regard is available at:

http://darpg.gov.in/darpgwebsite_cms/Document/file/CSMeOP_1st_Edition.pdf.

3. Objective

3.1 The objective of this policy is to ensure secure access and usage of Government of India e-mail services by its users. Users have the responsibility to use this resource in an efficient, effective, lawful, and ethical manner. Use of the Government of India e-mail service amounts to the user's agreement to be governed by this policy.

3.2 All services under e-mail are offered free of cost to all officials under Ministries / Departments / Statutory Bodies / Autonomous bodies (henceforth referred to as "Organization [3]" in the policy) of both Central and State/UT Governments. More information is available under "NIC e-mail Services and Usage Policy" at http://www.deity.gov.in/content/policiesguidelines/ under the caption "E-mail Policy".

3.3 Any other policies, guidelines or instructions on e-mail previously issued shall be superseded by this policy.

4. Roles specified for implementation of the Policy

The following roles are specified in each organization using the GoI e-mail service. The official identified for the task shall be responsible for the management of the entire user base configured under that respective domain.

4.1 Competent Authority[4] as identified by each organization

4.2 Designated nodal officer[5] as identified by each organization

4.3 GoI e-mail service Implementing Agency (IA), i.e. National Informatics Centre or the exempt organisation as per Clause 14 of this policy.

5. Basic requirements of GoI e-mail Service

5.1 Security

a) Considering the security concerns with regard to a sensitive deployment like e-mail, apart from the service provided by the IA, there would not be any other e-mail service under GoI.

b) All organizations, except those exempted under clause 14 of this policy, should migrate their e-mail services to the centralized deployment of the IA for security reasons and uniform policy enforcement. For the purpose of continuity, the e-mail address of the organization migrating their service to the IA deployment shall be retained as part of the migration process. Wherever it is technically feasible, data migration shall also be done.

c) Secure access to the GoI email service

i) It is recommended for users working in sensitive offices to use VPN[7]/OTP[8] for secure authentication as deemed appropriate by the competent authority.

ii) It is recommended that GoI officials on long deputation/stationed abroad and handling sensitive information should use (VPN)/ (OTP) for accessing GoI e-mail services as deemed appropriate by the competent authority.

iii) It is recommended that Embassies and missions abroad should use Static IP addresses for accessing the services of the IA as deemed appropriate by the competent authority.

iv) More information is available under “Guidelines for E-mail Management and Effective E-mail Usage” at http://www.deity.gov.in/content/policiesguidelines under the caption “E-mail Policy”.

d) From the perspective of security, the following shall be adhered to by all users of GoI e-mail service:

i) Relevant Policies framed by Ministry of Home Affairs, relating to classification, handling and security of information shall be followed.

ii) Use of Digital Signature Certificate (DSC) [6] and encryption shall , be mandatory for sending e-mails deemed as classified and sensitive, in accordance with the relevant policies of Ministry of Home Affairs. Updation of current mobile numbers under the personal profile of users is mandatory for security reasons. The number would be used only for alerts and information regarding security sent by the IA. Updation of personal e-mail id (preferably from a service provider within India), in addition to the mobile number, shall also be mandatory in order to reach the user through an alternate means for sending alerts.

iii) Users shall not download e-mails from their official e-mail account, configured on the GoI mail server, by configuring POP [9] or IMAP [10] on any other e-mail service provider. This implies that users should not provide their GoI e-mail account details (id and password) to their accounts on private e-mail service providers.

iv) Any e-mail addressed to a user, whose account has been deactivated /deleted, shall not be redirected to another e-mail address. Such e-mails may contain contents that belong to the Government and hence no e-mails shall be redirected.

v) The concerned nodal officer of the organization shall ensure that the latest operating system, anti-virus and application patches are available on all the devices, in coordination with the User.

vi) In case a compromise of an e-mail id is detected by the IA, an SMS alert shall be sent to the user on the registered mobile number. In case an “attempt” to compromise the password of an account is detected, an e-mail alert shall be sent. Both the e-mail and the SMS shall contain details of the action to be taken by the user. In case a user does not take the required action even

after five such alerts (indicating a compromise), the IA reserves the right to reset the password of that particular e-mail id under intimation to the nodal officer of that respective organization.

vii) In case of a situation when a compromise of a user id impacts a large user base or the data security of the deployment, the IA shall reset the password of that user id. This action shall be taken on an immediate basis, and the information shall be provided to the user and the nodal officer subsequently. SMS shall be one of the prime channels to contact a user; hence all users should ensure that their mobile numbers are updated.

viii) Forwarding of e-mail from the e-mail id provided by GoI to the Government official's personal id outside the GoI e-mail service is not allowed due to security reasons. Official e-mail id provided by the IA can be used to communicate with any other user, whether private or public. However, the user must exercise due discretion on the contents that are being sent as part of the e-mail.

ix) Auto-save of password in the Government e-mail service shall not be permitted due to security reasons.

x) More details regarding security measures are available in "NIC Security Policy" at http://www.deity.gov.in/content/policiesguidelines under the caption "E-mail Policy".

xi) The guidelines for effective e-mail usage have been described in "Guidelines for E-mail Account Management and Effective E-mail Usage" available at http://www.deity.gov.in/content/policiesguidelines under the caption "Email Policy".

5.2 E-mail Account Management

a) Based on the request of the respective organizations, IA will create two ids, one based on the designation and the other based on the name. Designation based id's are recommended for officers dealing with the public. Use of alphanumeric characters as part of the e-mail id is recommended for sensitive users as deemed appropriate by the competent authority.

b) Government officers who resign or superannuate after rendering at least 20 years of service shall be allowed to retain the name based e-mail address i.e. userid@gov.in for one year post resignation or superannuation. Subsequently, a new e-mail address with the same user id but with a different domain address (for instance, userid@pension.gov.in), would be provided by the IA for their entire life.

More details pertaining to e-mail account management are provided in "Guidelines for E-mail Account Management and Effective E-mail Usage"" available at http://www.deity.gov.in/content/policiesguidelines under the caption "Email Policy". The document covers creation of E-mail addresses, process of account creation, process of handover of designation-based ids, status of account after resignation and superannuation, data retention & backup and deactivation of accounts.

5.3 Delegated Admin Console

Organizations can avail the "Delegated Admin Console" service from IA. Using the console the authorized person of an organization can create/delete/change the password of user ids under that respective domain as and when required without routing the request through IA. Organizations that do not opt for the admin console need to forward their requests with complete details to the IA's support cell (support@gov.in).

5.4 E-mail Domain & Virtual Hosting

a) GoI provides virtual domain hosting for e-mail. If an organization so desires, the IA can offer a domain of e-mail addresses as required by them. This implies that if an organization requires an address resembling the website that they are operating, IA can provide the same.

b) By default, the address "userid@gov.in" shall be assigned to the users. The user id shall be created as per the addressing policy available at http://www.deity.gov.in/content/policiesguidelines/ under "E-mail Policy".

C) Organizations desirous of an e-mail address belonging to other domains (e.g. xxxx@deity.gov.in, yyyy@tourism.gov.in) need to forward their requests to the IA

5.5 Use of Secure Passwords

All users accessing the e-mail services must use strong passwords for security of their e-mail accounts. More details about the password policy are available in "Password Policy" at http://www.deity.gov.in/content/policiesguidelines under the caption "E-mail Policy".

5.6 Privacy

Users should ensure that e-mails are kept confidential. IA shall take all possible precautions on maintaining privacy. Users must ensure that information regarding their password or any other personal information is not shared with anyone.

6. Responsibilities of User Organizations

6.1 Policy Compliance

a) All user organizations shall implement appropriate controls to ensure compliance with the e-mail policy by their users. IA shall give the requisite support in this regard.

b) The user organizations shall ensure that official e-mail accounts of all its users are created only on the e-mail server of the IA**.**

c) Nodal officer of the user organization shall ensure resolution of all incidents related to the security aspects of the e-mail policy. IA shall give the requisite support in this regard.

d) Competent Authority of the user organization shall ensure that training and awareness programs on e-mail security are organized at regular intervals. Implementing Agency shall provide the required support.

6.2 Policy Dissemination

a) Competent Authority of the concerned organization should ensure dissemination of the e-mail policy.

b) Competent Authority should use Newsletters, banners, bulletin boards etc, to facilitate increased awareness on the e-mail policy.

c) Orientation programs for new recruits shall include a session on the e-mail policy.

7. Responsibilities of Users

7.1 Appropriate Use of E-mail Service

a) E-mail is provided as a professional resource to assist users in fulfilling their official duties. Designation based ids should be used for official communication and name based ids can be used for both official and personal communication.

b) Examples of inappropriate use of the e-mail service

i) Creation and exchange of e-mails that could be categorized as harassing, obscene or threatening.

ii) Unauthorized exchange of proprietary information or any other privileged, confidential or sensitive information.

iii) Unauthorized access of the services. This includes the distribution of e-mails anonymously, use of other officers' user ids or using a false identity.

iv) Creation and exchange of advertisements, solicitations, chain letters and other unofficial, unsolicited e-mail.

v) Creation and exchange of information in violation of any laws, including copyright laws.

vi) Wilful transmission of an e-mail containing a computer virus.

vii) Misrepresentation of the identity of the sender of an e-mail.

viii) Use or attempt to use the accounts of others without their permission.

ix) Transmission of e-mails involving language derogatory to religion, caste, ethnicity, sending personal e-mails to a broadcast list, exchange of e-mails containing anti-national messages, sending e-mails with obscene material, etc.

x) Use of distribution lists for the purpose of sending e-mails that are personal in nature, such as personal functions, etc.

Any case of inappropriate use of e-mail accounts shall be considered a violation of the policy and may result in deactivation [11] of the account. Further, such instances may also invite scrutiny by the investigating agencies depending on the nature of violation.

7.2 User's Role

a) The User is responsible for any data/e-mail that is transmitted using the GoI e-mail system. All e-mails/data sent through the mail server are the sole responsibility of the user owning the account.

b) Sharing of passwords is prohibited.

c) The user's responsibility shall extend to the following:

i) Users shall be responsible for the activities carried out on their client systems, using the accounts assigned to them.

ii) The 'reply all' and the use of 'distribution lists' should be used with caution to reduce the risk of sending e-mails to wrong people.

iii) Back up of important files shall be taken by the user at regular intervals. The IA shall not restore the data lost due to user's actions.

8. Service Level Agreement

The IA shall provide the e-mail services based on the Service Level Agreement (SLA) available at http://www.deity.gov.in/content/policiesguidelines under the caption "E-mail Policy".

9. Scrutiny of e-mails/Release of logs

9.1 Notwithstanding anything in the clauses above, the disclosure of logs/e-mails to law enforcement agencies and other organizations by the IA would be done only as per the IT Act 2000 and other applicable laws.

9.2 The IA shall neither accept nor act on the request from any other organization, save as provided in this clause, for scrutiny of e-mails or release of logs.

9.3 IA will maintain logs for a period of two years.

10. Security Incident Management Process

10.1 A security incident is defined as any adverse event that can impact the availability, integrity, confidentiality and authority of Government data. Security incidents can be due to factors like malware, phishing [12], loss of a device, compromise of an e-mail id etc.

10.2 It shall be within the right of the IA to deactivate or remove any feature of the e-mail service if it is deemed as a threat and can lead to a compromise of the service.

10.3 Any security incident, noticed or identified by a user must immediately be brought to the notice of the Indian Computer Emergency Response Team (ICERT) and the IA.

11. Intellectual Property

11.1 Material accessible through the IA's e-mail service and resources may be subject to protection under privacy, publicity, or other personal rights and intellectual property rights, including but not limited to, copyrights and laws protecting patents, trademarks, trade secrets or other proprietary information. Users shall not use the Government service and resources in any manner that would infringe, dilute, misappropriate, or otherwise violate any such rights.

12. Enforcement

12.1 This "E-mail policy" is applicable to all Government employees as specified in clause 2.2.

12.2 Each organization shall be responsible for ensuring compliance with the provisions of this policy. The Implementing Agency would provide necessary technical assistance to the organizations in this regard.

13. Deactivation

13.1 In case of threat to the security of the Government service, the e-mail id being used to impact the service may be suspended or deactivated immediately by the IA.

13.2 Subsequent to deactivation, the concerned user and the competent authority of that respective organization shall be informed.

14. Exemption

14.1 Organizations, including those dealing with national security, that currently have their own independent mail servers can continue to operate the same, provided the e-mail servers are hosted in India. These organizations however need to ensure that the principles of the e-mail policy are followed. However, in the interest of uniform policy enforcement and security, it is recommended that these organizations should consider migrating to the core service of the IA.

14.2 Indian Missions and Posts abroad may, however, maintain alternative e-mail services hosted outside India to ensure availability of local communication channels under exigent circumstances such as disruption of internet services that can cause non-availability of Government e-mail services.

14.3 Organizations operating Intranet [13] mail servers with air-gap are exempted from this policy.

15. Audit of E-mail Services

The security audit of NIC email services and other organizations maintaining their own mail server shall be conducted periodically by an organization approved by Deity.

16. Review

Future changes in this Policy, as deemed necessary, shall be made by DeitY with approval of the Minister of Communication & IT after due inter-ministerial consultations.

GLOSSARY

S.No	TERM	DEFINITION
1	**Users**	Refers to Government/State/UT employees who are accessing the Government e-mail services.
2	**Implementing agency (IA)**	For the purpose of this policy, the implementing agency is "National Informatics Centre" under the Department of Electronics and Information Technology, Ministry of Communications and Information Technology, Government of India
3	**Organization**	For the purpose of this policy, organisation refers to all ministries/departments/offices/statutory bodies/autonomous bodies, both at the Central and State level. Government organizations offering commercial services are not included.
4	**Competent Authority**	Officer responsible for taking and approving all decisions relating to this policy in his Organization
5.	**Nodal Officer**	Officer responsible for all matters relating to this policy who will coordinate on behalf of the Organization
6	**DSC**	A **digital signature** is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives the recipient reason to believe that the e-mail was created by a known sender, such that the sender cannot deny having sent the e-mail (authentication and non-repudiation) and that the e-mail was not altered in transit (integrity).
7	**VPN**	A **virtual private network** extends a private network across a public network, such as the Internet. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private network, while benefitting from the functionality, security and management policies of the private network
8	**OTP**	A **one-time password** (OTP) is a password that is valid for only one login session or transaction. OTPs avoid a number of shortcomings that are associated with traditional (static) passwords
9	**POP**	**POP i**s short for **P**ost **O**ffice **P**rotocol, a protocol used to retrieve e-mail from a mail server.
10	**IMAP**	IMAP is short for **"The Internet Message Access Protocol",** a protocol used to retrieve e-mail from a remote mail server. Unlike POP, in IMAP, Messages are displayed on your local computer but are kept and stored on the mail server. IMAP allows you to sync your folders with the e-mail server which is not possible using POP.

11	**Deactivation**	**Deactivation** of an account means that the account can no longer be accessed. All e-mails sent to a deactivated account shall bounce to the sender
12	**Phishing**	**Phishing** is a fraudulent attempt, usually made through e-mail, to steal a user's personal information. Phishing e-mails almost always tell a user to click a link that takes the user to a site from where the personal information is requested. Legitimate organisations would never request this information via e-mail. Users should never click on a link. A user should always type a URL in the browser even if the link appears genuine**.**
13	**Intranet**	An intranet is a private network that is contained within an organization. For the purpose of this policy, computers connected to an intranet are not allowed to connect to internet.